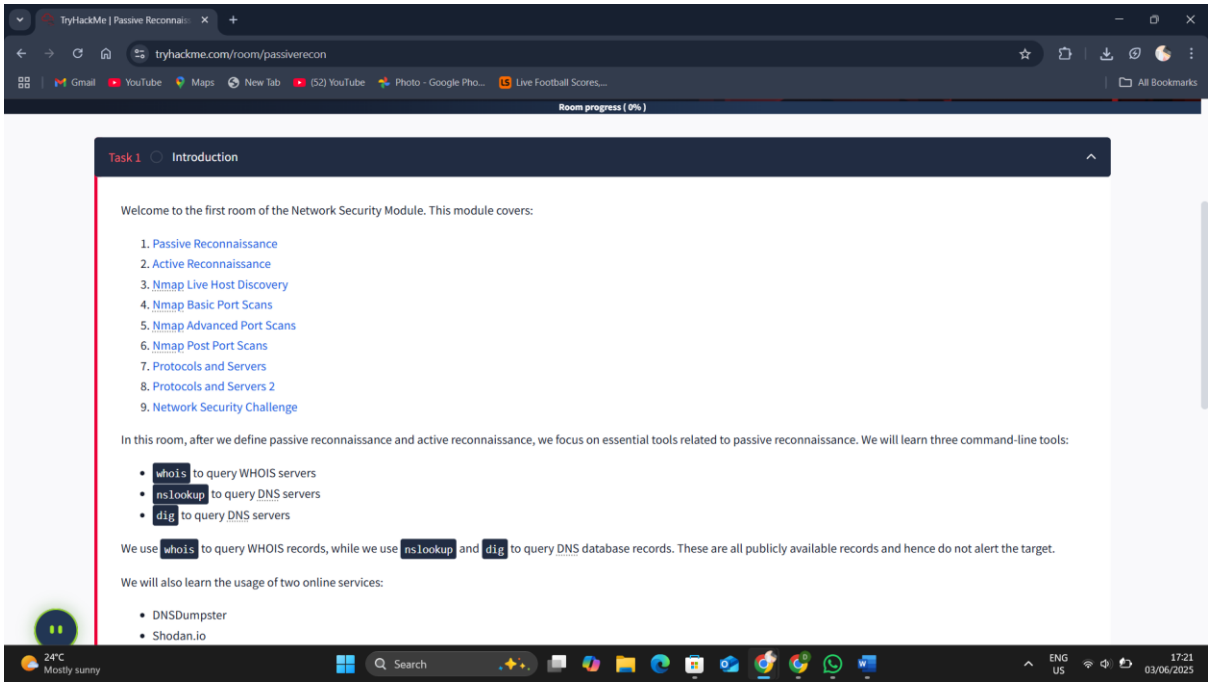
NAME:	**GRAHAM DESCENT OYIGO**
GMAIL:	**grahamoyigo19@gmail.com**
ADMISSION NUMBER:	**cs-sa10-25023**
MODULE:	**PASSIVE RECONNAISSANCE: TRYHACKME**
COMPLETION LINK:	https://tryhackme.com/p/grahamoyigo19?show_achievem

Passive Reconnaissance: TryHackMe

This report details the key learnings from the Passive Reconnaissance" room on TryHackMe, outlining various techniques and tools used to gather information about a target without directly interacting with it.

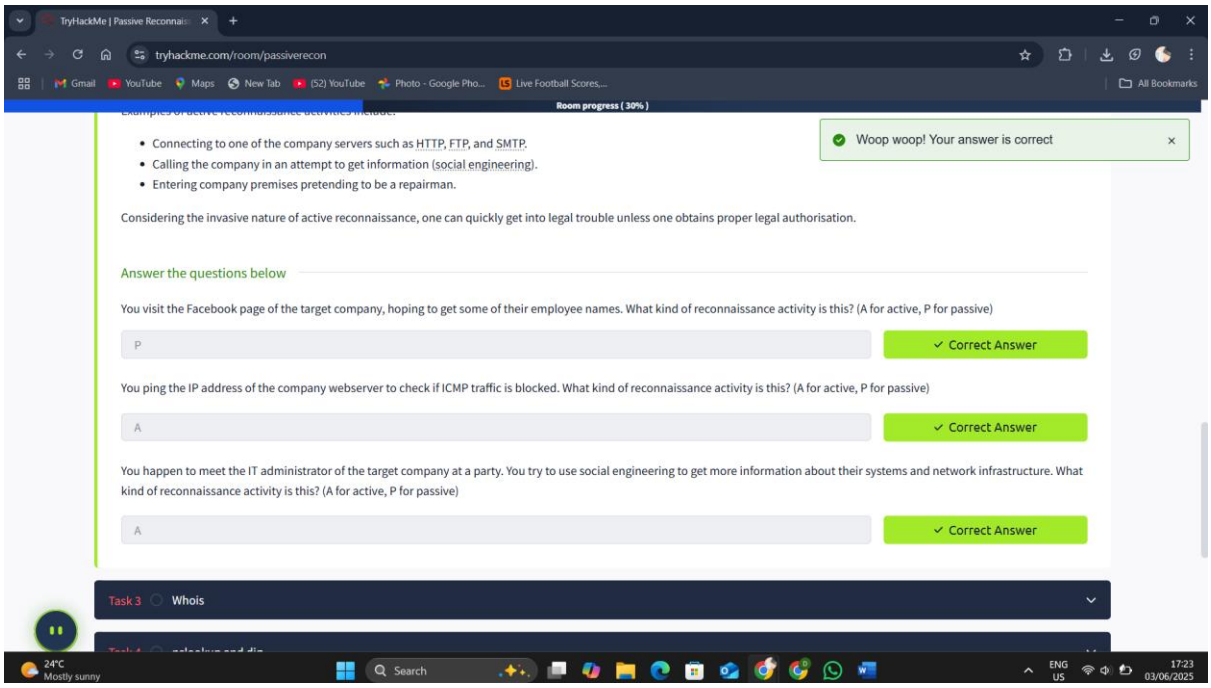
Task 1: Introduction

In this introductory task, I learned about the scope of the Network Security Module, which includes both passive and active reconnaissance. The focus of this particular room is on passive reconnaissance, specifically covering essential command-line tools like whois, nslookup, and dig for querying public WHOIS and DNS records. Additionally, I was introduced to online services such as DNSDumpster and Shodan.io, which facilitate information gathering without direct interaction with the target. The task also highlighted the prerequisites of basic networking and command-line knowledge.



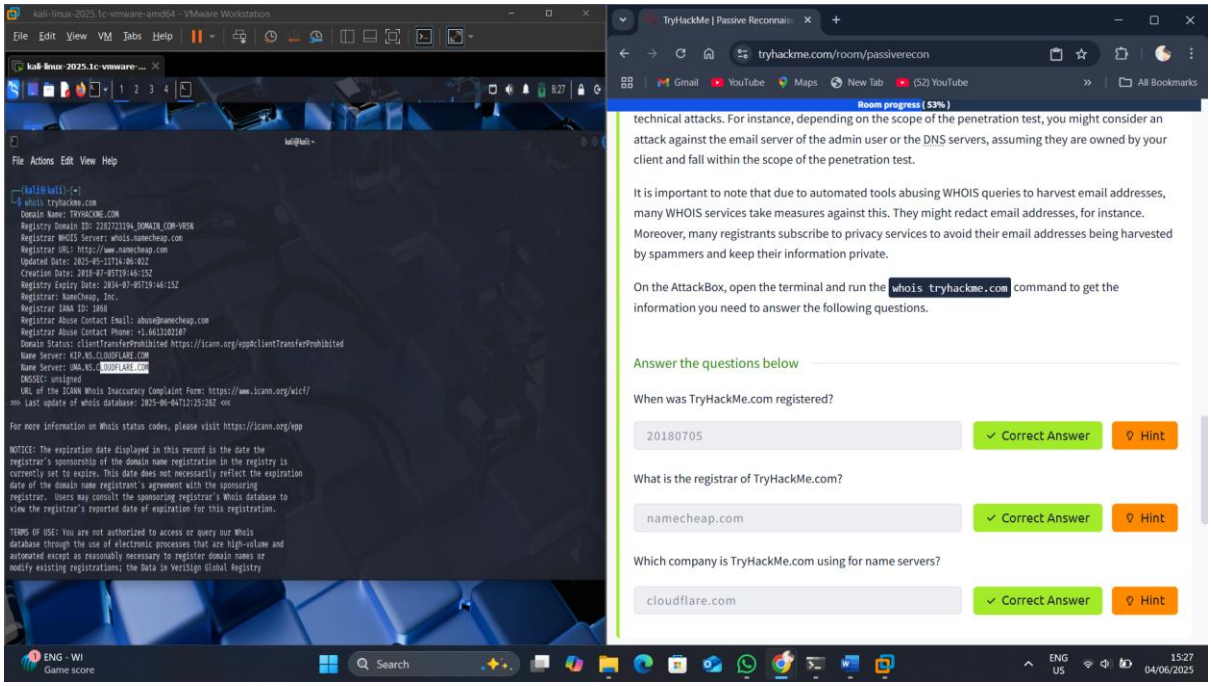
Task 2: Passive Versus Active Recon

This section clarified the fundamental difference between passive and active reconnaissance. Passive reconnaissance involves gathering information about a target without direct engagement, relying on publicly available data such as DNS records, job postings, or news articles. This method is discreet and does not alert the target. In contrast, active reconnaissance requires direct interaction with the target, such as connecting to servers, social engineering, or physical intrusion. Due to its invasive nature, active reconnaissance carries significant legal risks if not conducted with proper authorization.



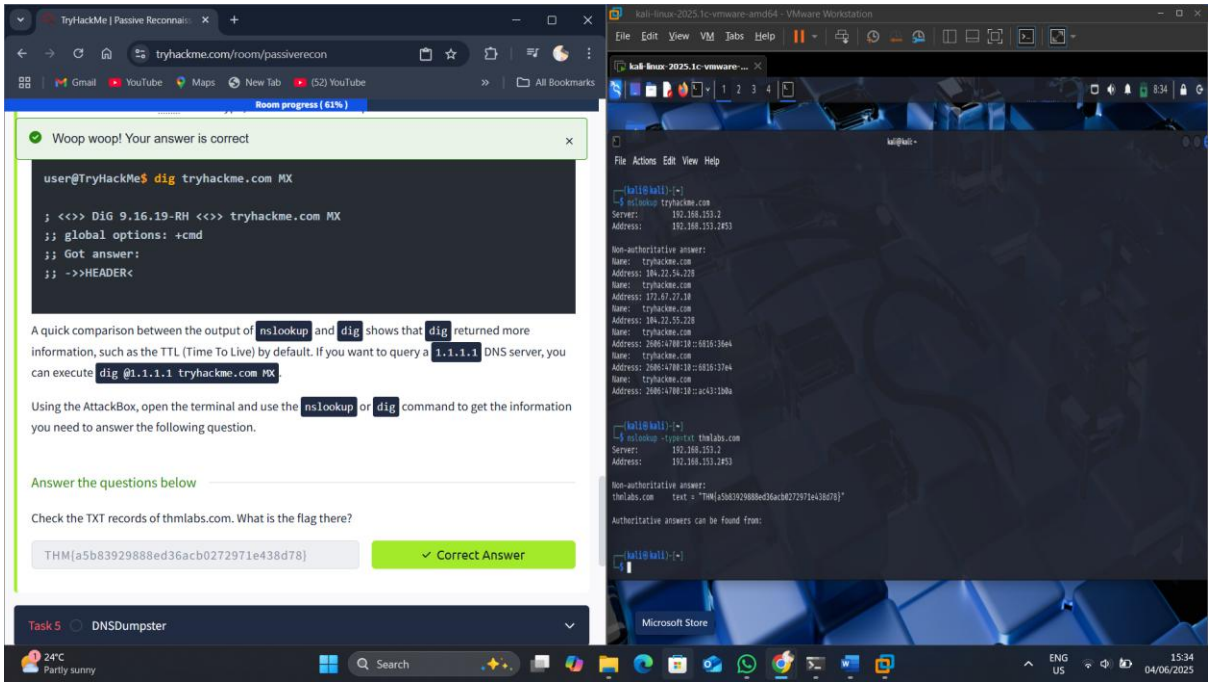
Task 3: Whois

In this task, I learned about the WHOIS protocol, which operates on TCP port 43 and is used to query domain registrars for information about registered domain names. Key data points obtainable from WHOIS records include the registrar, contact information for the registrant (though often redacted for privacy), creation, update, and expiration dates of the domain, and the associated name servers. I also learned how to use the whois command-line client with the syntax whois DOMAIN_NAME to retrieve this public information. This data is valuable for identifying potential attack surfaces, such as email servers for social engineering or DNS servers for technical attacks, while also noting that privacy services and redaction efforts can limit the amount of publicly available contact information.



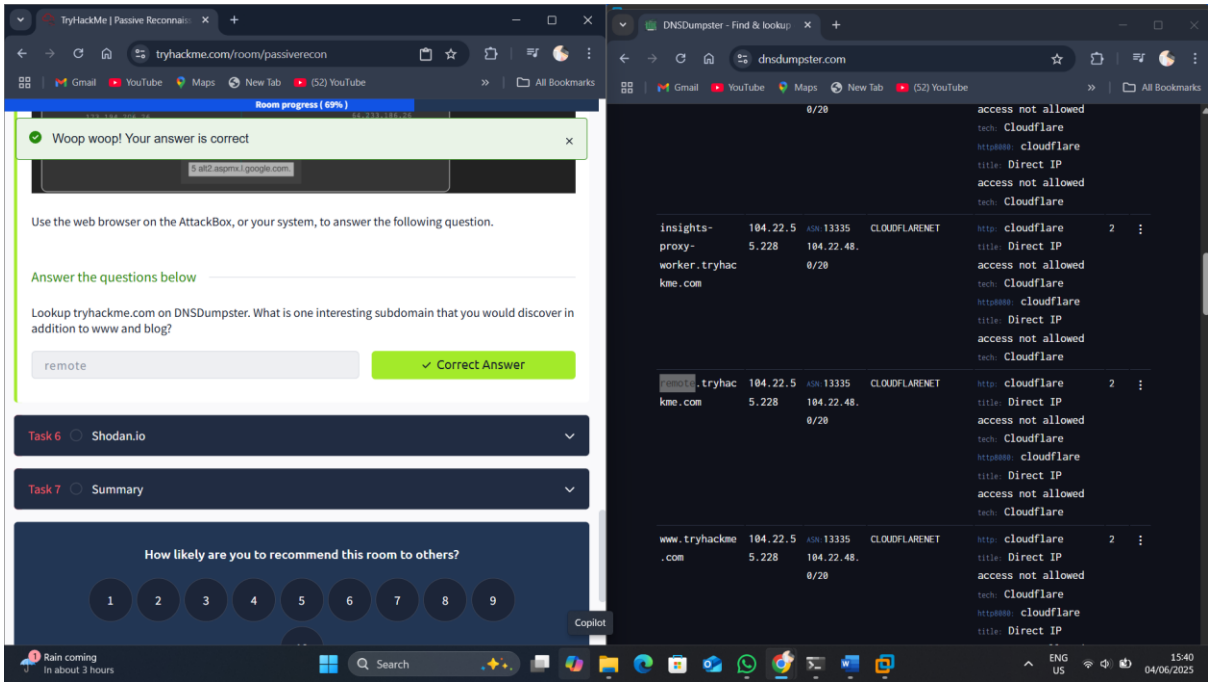
Task 4: nslookup and dig

This task introduced me to nslookup (Name Server Look Up) and dig (Domain Information Groper), two command-line tools for querying DNS servers. I learned how to use nslookup to find the IP addresses (IPv4 and IPv6) of a domain using A and AAAA record types, respectively, and how to query specific DNS servers like Cloudflare's 1.1.1.1. The utility of nslookup for retrieving MX (Mail Exchanger) records was also demonstrated, showing how to identify a domain's email server configuration, which can be crucial for reconnaissance. Furthermore, I explored dig as a more advanced alternative, noting its ability to provide more detailed DNS information, such as TTL (Time To Live) values, by default. Both tools are essential for gathering passive intelligence about a target's network infrastructure.



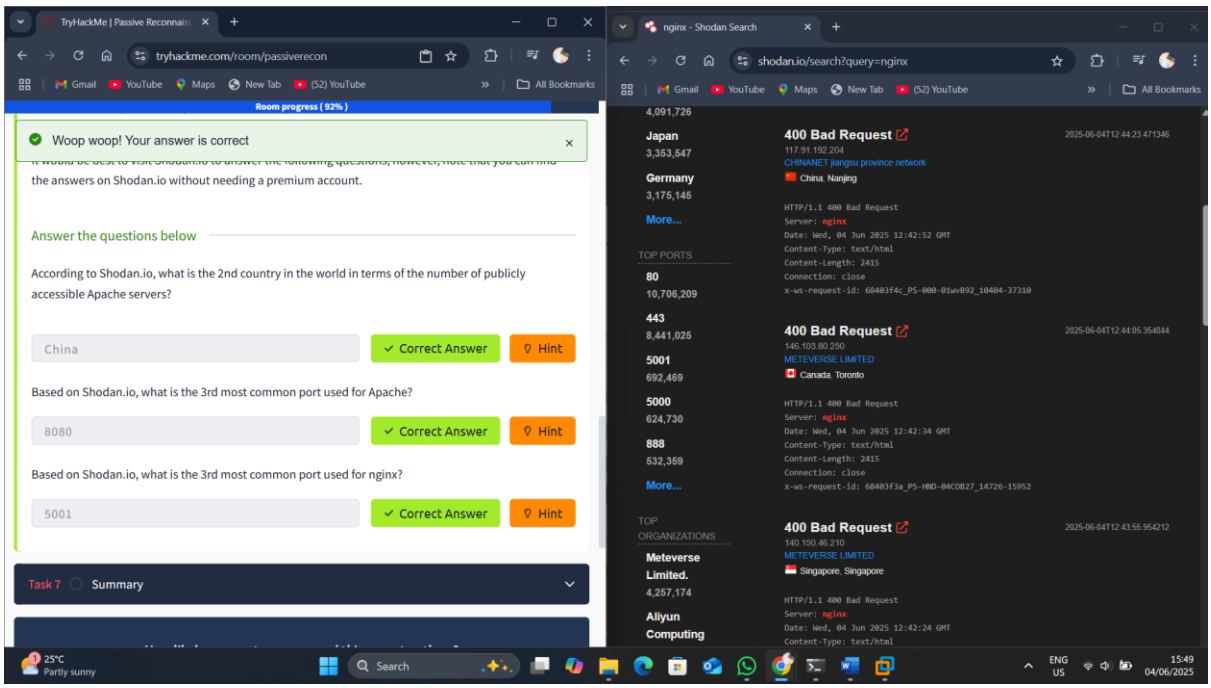
Task 5: DNSDumpster

In this task, I learned about DNSDumpster, an online service that significantly simplifies the process of discovering subdomains and comprehensive DNS information that might be difficult to uncover with basic nslookup or dig queries alone. DNSDumpster aggregates publicly known DNS records, including subdomains, and presents them in easy-to-read tables and graphical formats. This tool provides resolved IP addresses, geolocation data, detailed MX records with associated server information, and TXT records, offering a rich overview of a target's DNS footprint from a single query. This capability is invaluable for identifying potentially vulnerable or unadvertised subdomains.



Task 6: Shodan.io

In this task, I learned about Shodan.io, a search engine for internet-connected devices, contrasting it with traditional search engines for web pages. Shodan actively connects to online devices, collects information about their services, and makes this data searchable. This allows for passive reconnaissance by revealing details such as IP addresses, hosting companies, geographic locations, and server types and versions without direct interaction with the target. Shodan.io is useful for both offensive security (identifying potential attack surfaces) and defensive security (understanding an organization's exposed assets).



Task 7: Summary

This final section summarized the core concepts of passive reconnaissance covered in the room. I reinforced my understanding of command-line tools like whois, nslookup, and dig for querying public records, and the utility of online services such as DNSDumpster and Shodan.io for gathering extensive information without direct target interaction. The summary also highlighted the significant potential of these tools to uncover valuable intelligence once their functionalities and output interpretation are mastered.

Purpose	Command-line Example
Lookup WHOIS record	whois tryhackme.com
Lookup DNS A records	nslookup -type=A tryhackme.com
Lookup DNS MX records at DNS server	nslookup -type=MX tryhackme.com 1.1.1.1
Lookup DNS TXT records	nslookup -type=TXT tryhackme.com
Lookup DNS A records	dig tryhackme.com A
Lookup DNS MX records at DNS server	dig @1.1.1.1 tryhackme.com MX
Lookup DNS TXT records	dig tryhackme.com TXT